TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. T00001-0466-US

In Re Application Of: **PROOS, John A. et al.**

Serial No.	Filing Date	Examiner	Group Art Unit
10/734,231	December 15, 2003	Not yet assigned	2131

Title: **METHOD AND APPARATUS FOR PROTECTING NTRU AGAINST A TIMING ATTACK**

Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), provided that the Information Disclosure Statement is filed before the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

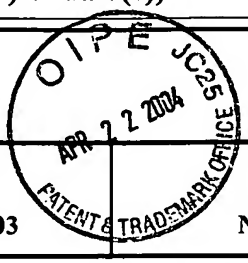
   ☐ the statement specified in 37 CFR 1.97(e);

   OR

   ☐ the fee set forth in 37 CFR 1.17(p).

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. T00001-0466-US

In Re Application: **PROOS, John A. et al.**



Serial No.	Filing Date	Examiner	Group Art Unit
10/734,231	December 15, 2003	Not yet assigned	2131

METHOD AND APPARATUS FOR PROTECTING NTRU AGAINST A TIMING ATTACK

Payment of Fee

(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

- ☐ A check in the amount of is attached.
- ☐ The Director is hereby authorized to charge and credit Deposit Account No. as described below.
  - ☐ Charge the amount of
  - ☐ Credit any overpayment.
  - ☐ Charge any additional fee required.

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (F:

_____
(Date)

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited on with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Certificate

***This certificate may only be used if paying by deposit account.**

Dated: 19 April 2004

Signature

John R.S. Orange (29,725)
McCarthy Tetrault LLP
Suite 4700, P.O. Box 48
66 Wellington Street West
Toronto Dominion Bank Tower
Toronto, ON M5K 1E6 Canada

Tel: 416 362-1812 Fax: 416 601-8454

cc:

ATTORNEY DOCKET NO.: **T00001-0466-US**
CUSTOMER NUMBER: **000027155**

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re patent application of:

PROOS, John A et al.

Serial No.:	**10/734,231**	Group Art Unit:	**2131**
Filed:	**December 15, 2003**	Examiner:	**NOT YET SPECIFIED**

Title: **METHOD AND APPARATUS FOR PROTECTING NTRU AGAINST A TIMING ATTACK**

Mail Stop DD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08B listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each document listed in the enclosed Form PTO/SB/08B is submitted herewith.

The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

This IDS is submitted pursuant to 37 CFR §1.97(b) and, accordingly, no fee is believed to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08B after being marked as being considered by the Examiner.

Respectfully submitted,

Date: 19 April 2007

John R.S. Orange
Registration No. **29,725**
Agent for Applicant

McCarthy Tétrault
Suite 4700, P.O. Box 48
Toronto Dominion Bank Tower
Toronto, Ontario M5K 1E6, Canada

Tel: 416 362-1812
Fax: 416 601-8454

PTO/SB/08B (06-03)
Approved for use through 06/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	10/734,231
Filing Date	December 15, 2003
First Named Inventor	PROOS
Group Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0466-US

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Consortium for Efficient Embedded Security, EESS #1: Implementation Aspects of NTRUEncrypt and NTRUSign, Version 1, November 2002.	
		HESS, E; JANSSEN, N; MEYER, B; SCHUETZE, T. "Information Leakage Attacks Against Smart Card Implementations of Cryptographic Algorithms and Countermeasures - A Survey", Proceedings of Eurosmart Security Conference, pp. 55-64, Marseilles, 2000, European Smart Card Industry Assoc., 2000.	
		SHAMIR, A. "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies", in Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2000, pp. 71-77, LNCS Vol. 1965, C.K. Koc et al, Eds., Springer-Verlag, 2000.	
		KOCHER, P.C. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", in Advances in Cryptology - CRYPTO'96, LNCS Vol. 1109, N. Koblitz, Ed., pp. 104-113, Springer-Verlag, 1996.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.